

Search:

vpn nortel



How can I configure the DI-604 or DI-614+ to allow me to use my Nortel Contivity VPN client?



Nortel Contivity will work with the DI-604 and DI-614+, however its functionality depends on the authentication type (AH will not work), NAT compatibility mode, and disabling keep alives on the server. Contact your Network Administrator to find out how your VPN is configured.

Step 1: Verify that you are using the latest version of firmware on your gateway.

[How do I update the firmware on my DI-604/614+?](#)

Step 2: Login to the Web Management for your router by entering its IP address (**192.168.0.1**) in your web browser. The default username is **admin**, and the password is blank.

Step 3: Click the **Advanced** Tab to access the Virtual Server Settings. There is a list of pre-defined Virtual Server Rules towards the bottom of the page. Find the IPSec Rule. Click the pen and paper icon to edit its settings. Enable the rule, enter the IP address of the computer attempting to connect to the VPN in the **Private IP** field, then **Apply** the changes.

[Windows98/ME IP Configuration](#)

[Windows2000/XP IP Configuration](#)

Virtual Servers List				Apply	Cancel	Help
Name	Private IP	Protocol	Schedule			
<input type="checkbox"/> Virtual Server FTP	0.0.0.0	TCP 21/21	always			
<input type="checkbox"/> Virtual Server HTTP	0.0.0.0	TCP 80/80	always			
<input type="checkbox"/> Virtual Server HTTPS	0.0.0.0	TCP 443/443	always			
<input type="checkbox"/> Virtual Server DNS	0.0.0.0	UDP 53/53	always			
<input type="checkbox"/> Virtual Server SMTP	0.0.0.0	TCP 25/25	always			
<input type="checkbox"/> Virtual Server POP3	0.0.0.0	TCP 110/110	always			
<input type="checkbox"/> Virtual Server Telnet	0.0.0.0	TCP 23/23	always			
<input type="checkbox"/> IPSec	0.0.0.0	UDP 500/500	always			
<input type="checkbox"/> PPTP	0.0.0.0	TCP 1723/1723	always			

Step 4: Create a new Virtual Server entry. Name the Virtual Server, "**NorteIVPN**". Enter the IP address of the computer attempting to connect to the VPN in the **Private IP** field. For the **Protocol Type**, select **Both**. Enter **9550** for both the **Public** and **Private Ports**. Set the **Schedule** to always, then **Apply** the settings.

Virtual Server

Applications

Filters

Firewall

DMZ

Home

Advanced

Tools

Status

Help

Virtual Server

Virtual Server is used to allow Internet users access to LAN services.

☒ Enabled
 ☐ Disabled

Name

NorteIVPN

Clear

Private IP

192.168.0.100

Protocol Type

Both

Private Port

9550

Public Port

9550

Schedule

☒ Always
 ☐ From time

00 : 00 AM to 00 : 00 AM

day Sun to Sun

Virtual Servers List

				Apply	Cancel	Help
Name	Private IP	Protocol	Schedule			
<input type="checkbox"/> Virtual Server FTP	0.0.0.0	TCP 21/21	always			
<input type="checkbox"/> Virtual Server HTTP	0.0.0.0	TCP 80/80	always			
<input type="checkbox"/> Virtual Server HTTPS	0.0.0.0	TCP 443/443	always			
<input type="checkbox"/> Virtual Server DNS	0.0.0.0	UDP 53/53	always			

Step 5: Access the **Tools** Page, then click the **Misc** button. **Disable** IPSec Pass-through, then click

Apply.

VPN Pass-Through

Allows VPN connections to work through the DI-604.

PPTP ☐ Enabled ☒ Disabled

IPSec ☐ Enabled ☒ Disabled

If the VPN Server is properly configured to work with clients behind NAT gateways you should be able to connect to the VPN.

All Contents © [D-Link Systems, Inc](#) 2001 | All Rights Reserved | [Terms of Use](#) | [Privacy Policy](#)
[Main Page](#) | [Products](#) | [Downloads](#) | [Registration](#) | [Training Guides](#) | [F.A.Q.](#) | [Contact](#)

Questions or problems regarding this web site should be directed to [Rnacinovich@azdot.gov].